le lab quantique

What we’ve achieved since Oct. 2018

3 Meetups

2 hackathons

1 major conference with BPI France (QCB)

1 event at Station F

A Meetup community > 500 members

Next ?

Projet submitted to the « Mission Fortezza » towards a National Plan on Quantum Technologies:

L'ambition du Lab Quantique est de placer la France sur la carte mondiale de sites d'excellence quantique en développant les liens étroits qui unissent acteurs académiques, industriels et investisseurs, en interaction avec le système d'innovation français

- Ecosystème
- Accélération
- Nouveau mode de coordination

Under the High Patronage of
Mr Emmanuel MACRON
President of the French Republic

THE FIRST GLOBAL GATHERING OF THE **DEEP TECH ECOSYSTEM**

Header – Deep Tech Week

DEEP
TECH
WEEK

9 | 13
MARCH 2020
PARIS

QUANTO NATION

CRYPTONEXT SECURITY

bpifrance

DEEP TECH WEEK

Quantum Cyber-Security : Impact And Challenges

March, 11th 2020 – 9h - 12h30

Bpifrance le HUB, 6-8 Bd Haussmann 75 009 Paris bpifrance

<Q|C|B>

QUANTUM COMPUTING BUSINESS

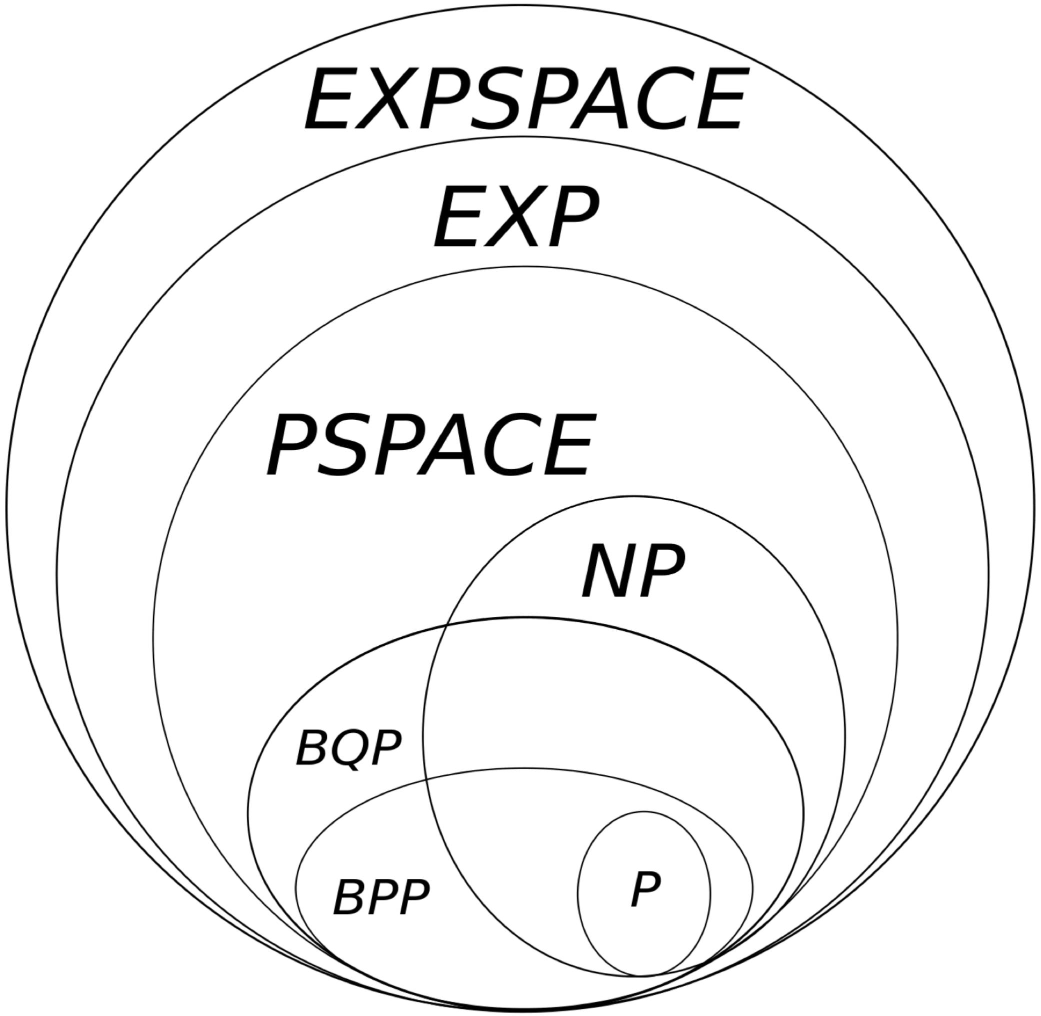
23/06/2020

Guest star: John Martinis

Quantum Algorithms

Leonard Wossnig
Chief Executive Officer

Why quantum?



Outlook for quantum algorithms in 2020

High level overview:

- ✓ (Quantum) algorithms are split in two different types:
  - Heuristics (variational optimizers like VQE, etc., QAOA, Annealing)
  - Algorithms with provable guarantees (QLSA, PE, Grover's, etc.)
- ✓ Different guarantees, requirements, and timelines apply
- ✓ Benchmarking versus proof: Yet, we neglect the overheads!
- ✓ Wide range of applications including




Content of the talk

1. Quantum computers today

2. Quantum algorithms with provable guarantees

3. Quantum Heuristics

4. Conclusion

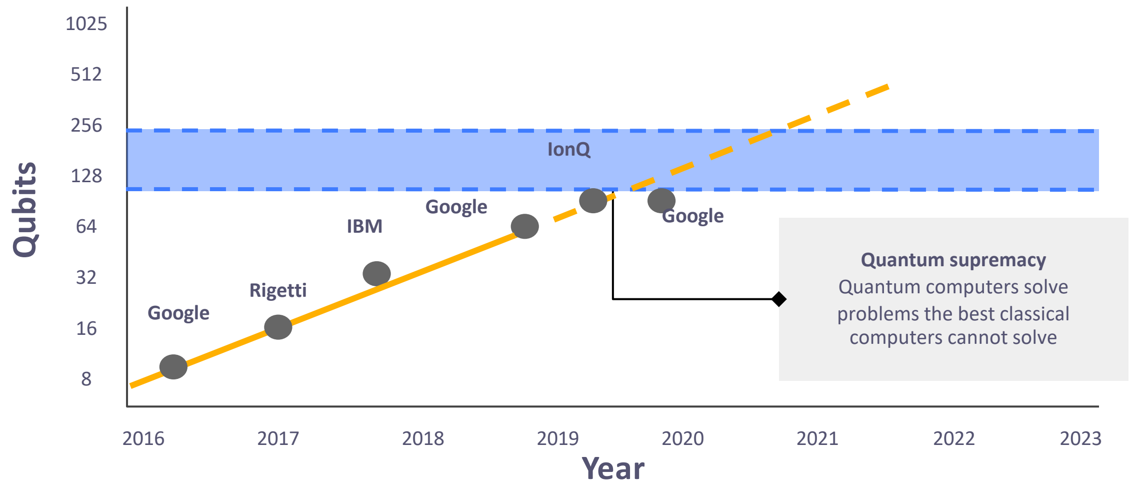
5. Rahko's approach

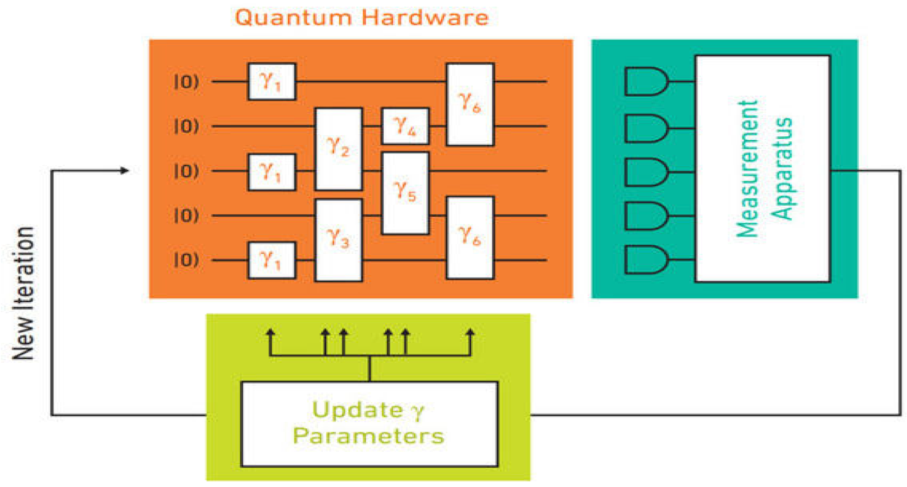
1
2
3
4
5

Quantum computers today

We are in the 'NISQ' era of quantum computing. This means:

- ✓ Noisy intermediate scale quantum computers
- ✓ Only a few quantum computers are available with a few qubits (currently ~53) each
- ✓ Qubits are hard to control, and no error correction possible
- ✓ Can only run Heuristic algorithms
- ✓ Can only use error mitigation





Algorithms with provable guarantees

Applications/Types:

- ✓ Algorithms based on Phase Estimation and Hamiltonian Simulation, for example linear systems, recommendation systems, SDPs, or chemistry simulations
- ✓ Algorithms based on Grover's (AA/AE)
- ✓ Algorithms for integer factorization, i.e., Shor's

Pros:

- ✓ Typically polynomial speedups and in certain cases up to exponential ones (Chem, Encrypt.)
- ✓ Inspired new classical algorithms

Cons:

Quantum Heuristics

Applications/Types:

- ✓ Simulation of chemistry and approximation of quantum states via VQE
- ✓ Machine learning, e.g. QGANs
- ✓ Optimization with e.g. QAOA
- ✓ Factoring and numerical (algebraic) operations with variational algorithms

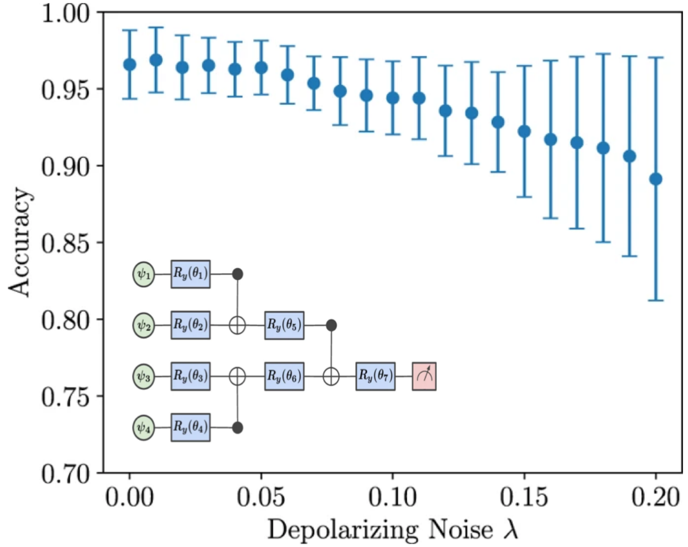
Pros:

- ✓ Promising first applications for some areas, such as quantum chemistry
- ✓ Algorithms can be run on current devices

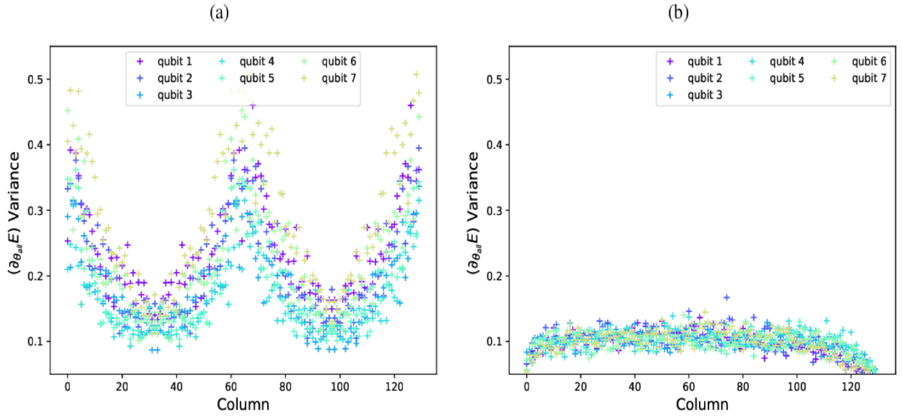
Cons:

- ✓ No theoretical guarantees possible, and unclear whether there is an advantage
- ✓ Scaling in particular is not entirely understood and larger-than-NISQ number of qubits likely required to be classically intractable (e.g. in optimization)

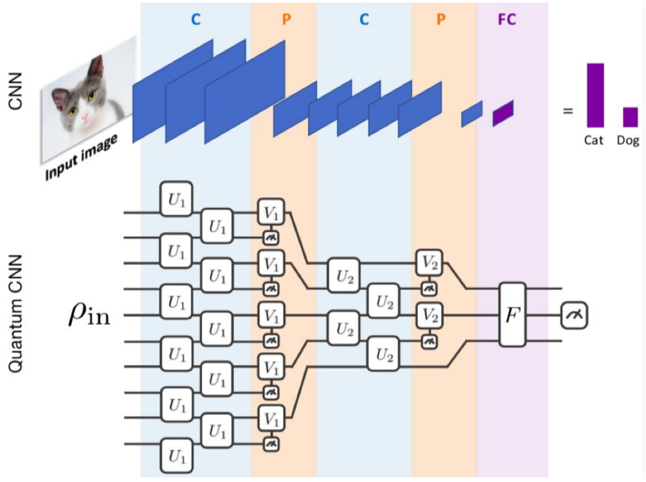
However, lots of interesting results!



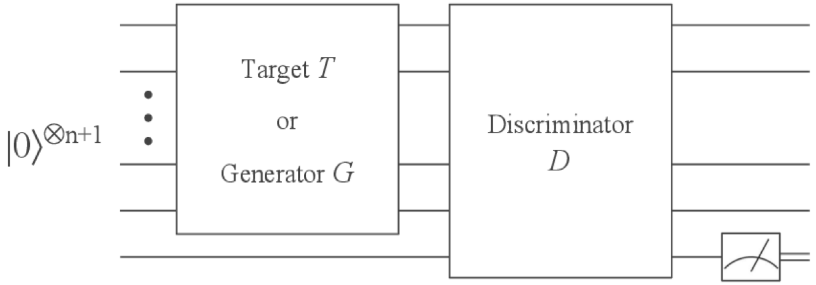
Grant *et al,* npj Quantum Information 2018

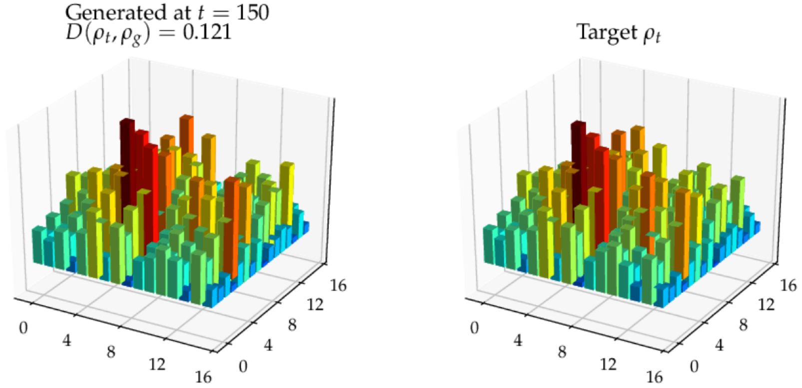


Grant *et al,* 2019

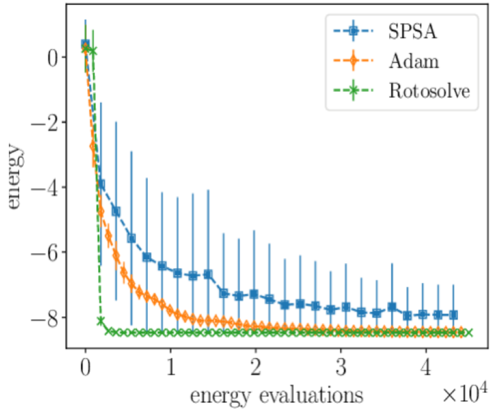


Cong *et al,* Nat Physics 2019





Benedetti *et al,* New Journal of Physics 2018



Ostaszewski *et al,* 2019

1
2
3
4
5

Conclusions

The good:

- ✓ Up to exponential advantages in the long term for chemistry applications
- ✓ Other advantages for ML, Optimisation, etc. possible
- ✓ Near term advantage possible
- ✓ Quantum inspired methods already useful today and used in industry

NISQ needs more work:

- ✓ Novel methods comparably to classical ones need to be developed in chemistry
- ✓ Better strategies to mitigate device errors necessary
- ✓ Better empirical understanding needed, e.g., scaling analysis etc.

Rahko's approach

We offer:

- ✓ QiML SaaS or on-premise software for fast chemistry simulation, reducing costs by up to 50%, e.g., for high-throughput screening
- ✓ Develop proof of concepts and long-term relationships with customers for NISQ and FECQ computation
- ✓ Education of customers about applications in chemistry, materials, and pharmaceuticals

rahko

AWS announced their partner program this month.
Rahko is one of the six partners and the only European one.
We work today with our customers to reduce their costs.

For more information - reach out to info@rahko.ai or see www.rahko.ai.

We are partnering with customers to solve their problems using quantum machine learning

CRYPTONEXT
SECURITY

We protect your data against the quantum computer

Ludovic Perret

ludovic.perret@cryptonext-security.com

Web site: www.cryptonext-security.com

Deep-tech founders

CTO
Jean-Charles Faugère, PhD, HDR, DR INRIA, Team leader
Cray & Atos Prizes
150 publications

CEO
Ludovic Perret, PhD,HDR

Atos prize
60 publications

COO
Frédéric de Portzamparc, PhD,

Formerly Strategic Marketing with tech start-up & Senior Security Consultant at Thales (Gemalto)

(External) R. P. Straub
Business strategy
Former Head of market development (ID Quantique)

R&D Team: 5 phd+internsphips

Agenda


le lab
quantique
Is Quantum Supremacy changing everything ?
Leonard Wossnig
CEO
rahko
Ludovic Perret
CEO
CRYPTONEXT
SECURITY
Sylvain Gigan
Co-Founder
LightOn

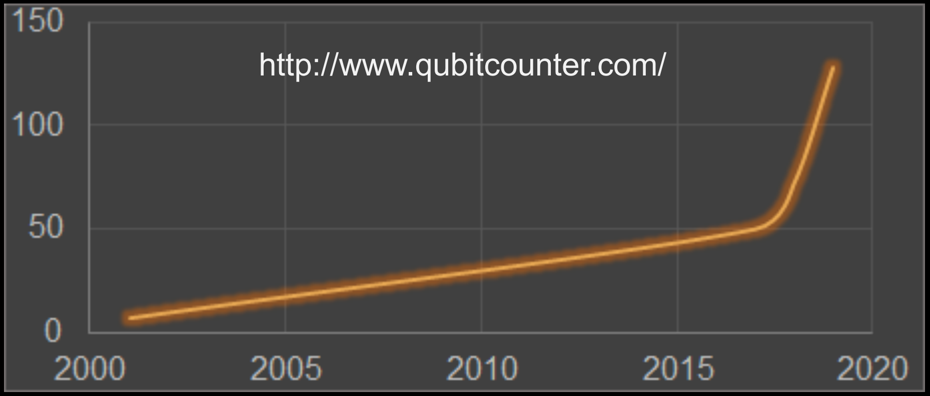
AGENDA

- Security Challenge
- Standardization Challenge
- Deployment Challenge

Security Challenge

Quantum computers are coming fast

- First versions commercially available today
- Exponential power increase since 1998

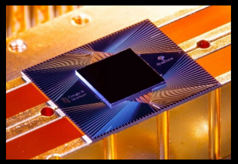


ATOS ANNOUNCES WORLD FIRST IN QUANTUM COMPUTING

Atos Quantum Learning Machine can now simulate real Qubits.

IBM Helps Researchers Explore the Impossible With New IBM Q System One

Hello quantum world! Google publishes landmark quantum supremacy claim



THE QUANTUM THREAT

Factoring $N = pq$ in $O(poly(\log N))$

Exhaustive search in $O(2^{n/2})$

COMPUTER	Time to break current standard (RSA-1024)
Classical	~ 400 years
Quantum	**< 1.2 h**

C. Gidney and M. Eker.
"How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits.", 2019.

ZAPATA

Variational Quantum Factoring (40 Bit, 2019) al

Consequences of Quantum Threat

- Sensitive data exposed
  - VPN links no more secure
- End of e-commerce
  - no more trust for on-line transactions
- Identity theft
  - Cryptocurrencies stolen
  - financial transactions
- Unauthorized remote access control
  - Planes, satellites, missiles, etc

Data are already at risk today

STANDARDIZATION CHALLENGE

RISK PERCEIVED AS MAJOR SINCE 2016

"Quantum risk is now simply too high and can no longer be ignored",

US National Institute of Standards and Technology, 2016

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

"For use cases requiring a long-lived protection of the information (≥ 20 years), it is advised to start taking the quantum threat into account."
"Enhance the crypto agility of existing products with quantum-safe cryptography, in order to facilitate the medium term transition."

ANSSI, 2018

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

« Plan National Quantique », leaded by P. Forteza (French gouvernement)

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

NEW QUANTUM-SAFE STANDARDS ARE IN DEFINITION

- *"Transition of US IT government infrastructure to a post-quantum cryptography will be completed by **2024**".*
- M. Scholl, NIST, 2017

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

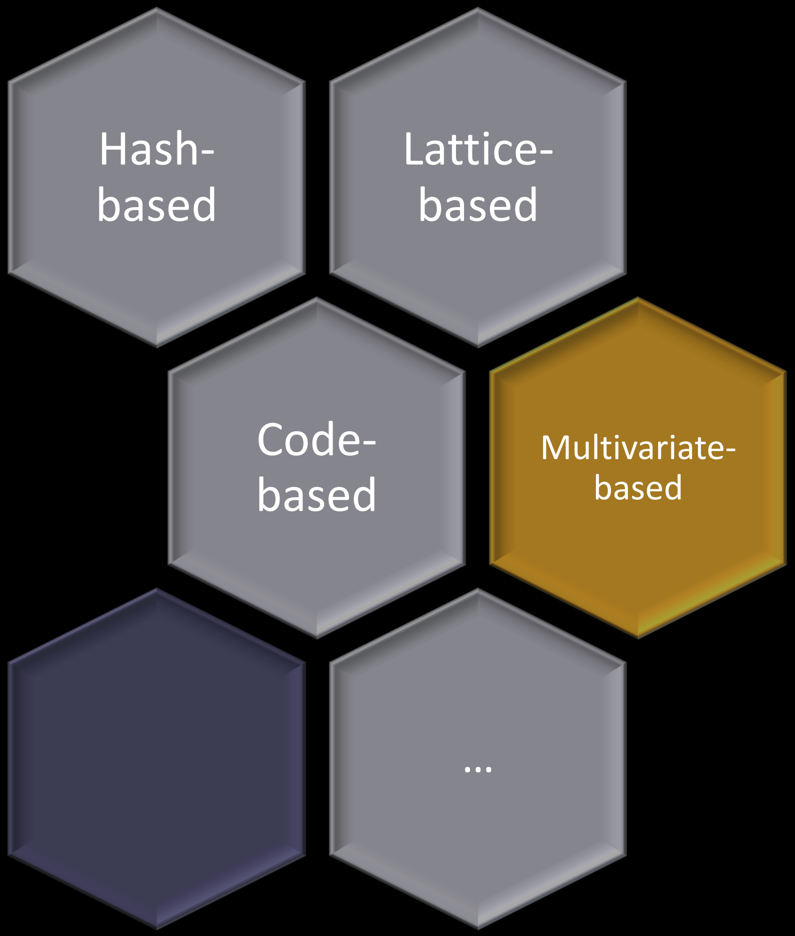
- Selection of cryptographic standards: NIST post-quantum competition
  - Several cryptographic functions standardized in **2022**
    - **Key-exchange and signature**

- China: a concurrent process, ending **end 2019**

Public-key cryptography : the core issue

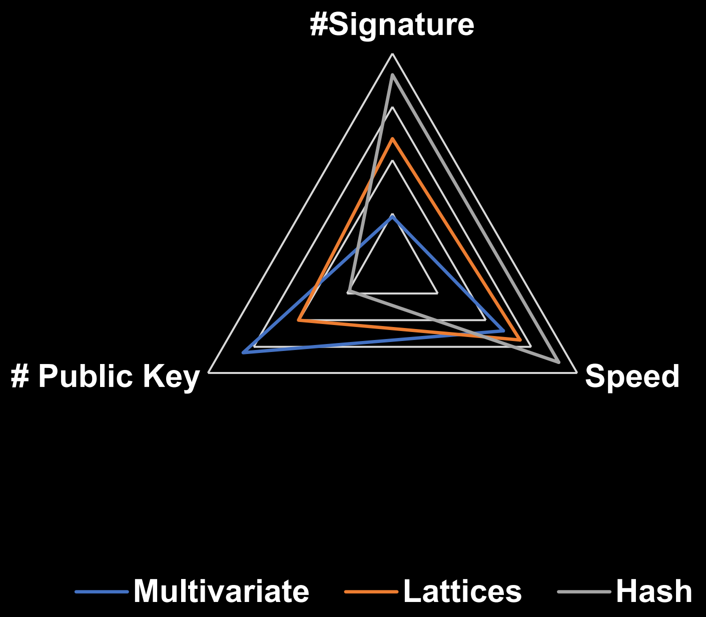
- Current public-key cryptographic standards are based on mathematical problems that are easy for a quantum computer
- New harder quantum-safe mathematical problems are currently evaluated by standardization bodies (NIST, ETSI, ISO, ….)
- Example : Multivariate crypto hard problem solving a system of non-linear equations

$$\begin{cases} x_1x_4 + x_1x_5 + x_2x_3 + x_2x_4 + x_3x_4 + x_4 + x_5 + 1 = 0 \\ x_1x_3 + x_1x_5 + x_2x_4 + x_3x_4 + x_3x_5 + x_2 + x_5 + 1 = 0 \\ x_1x_3 + x_1x_4 + x_1x_5 + x_2x_5 + x_3 + x_4 = 0 \\ x_1x_3 + x_1x_5 + x_2x_3 + x_2x_4 + x_2x_5 + x_3x_5 + x_4x_5 + x_1 + x_5 + 1 = 0 \\ x_1x_2 + x_1x_4 + x_1x_5 + x_2x_3 + x_2x_5 + x_3x_4 + x_4x_5 + x_1 = 0 \end{cases}$$



A GLOBAL EXPERTISE IS REQUIRED

- There is no ideal candidate for a drop-in replacement.
- Several standards will likely be defined in function of the application.
- Optimization is key for the deployment of upcoming quantum-safe standards into current security protocols.
- This requires a high-level expertise.

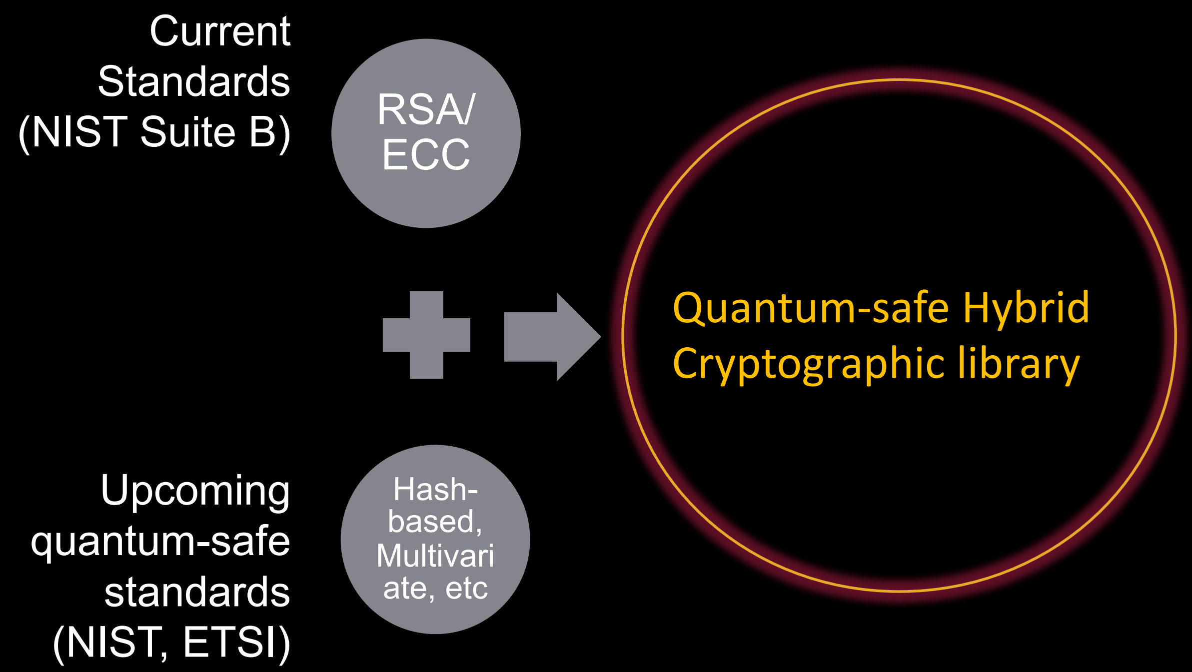


High level comparison for signatures schemes submitted to the NIST competition.

DEPLOYMENT CHALLENGE

CryptoNext: software that eliminates the quantum threat

- Ready for deployment today
- Smooth transition to quantum-safe
- Easy integration
- Transparent for final users
- Compliant with future standards



PRODUCTS

Cryptographic library (MVP)

Technological core of CryptoNext Security
Easy integration into security product/services (multiple vercicals)
Optimized : Efficient + available for multiple architectures (from PC → IOT)
On-going IP on secure implementations

Quantum-Safe VPN (2021)

- Security product build on top of the library
- Protect communication for the long term
- To be certified by a national security security agency (ANSSI, France)

CONSULTING/STUDY → POC/POV → LICENSE

REAL-LIFE DEPLOYMENT OF CRYPTONEXT SOFTWARE IN 2016

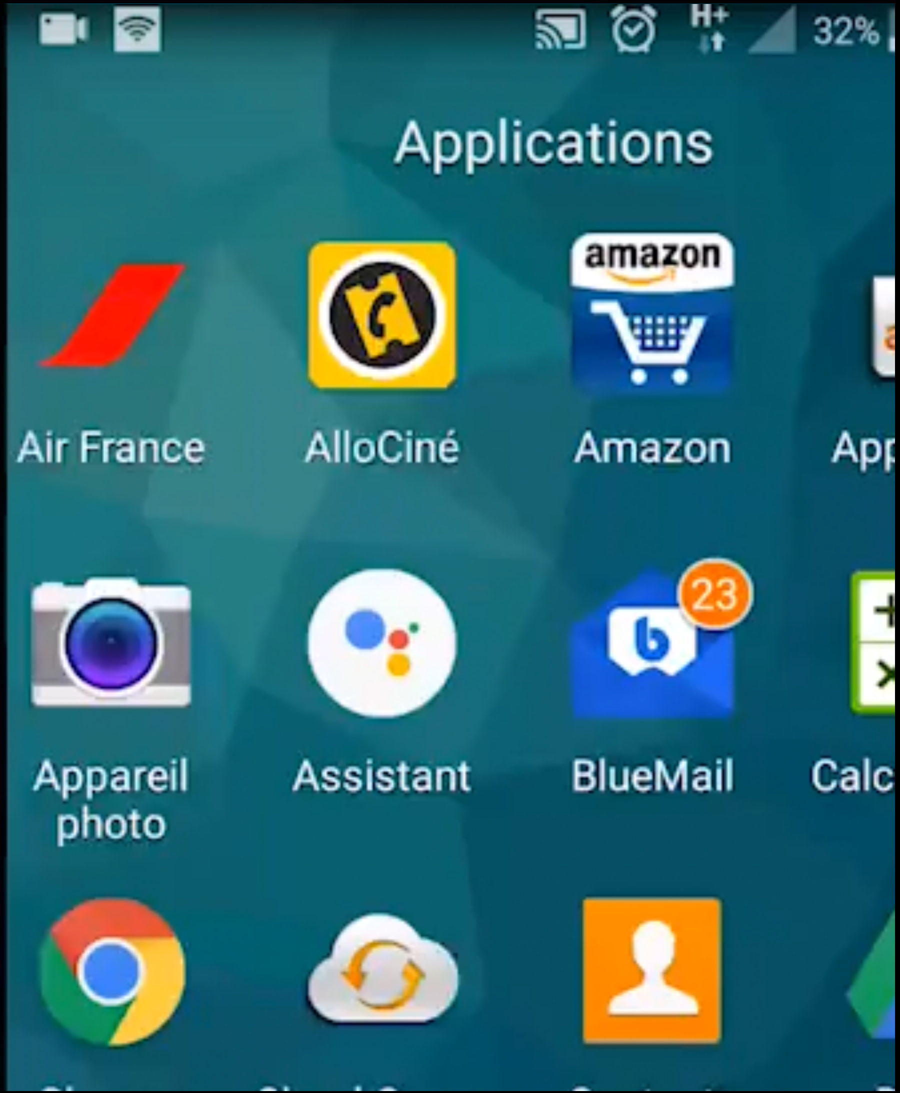
- Successful MVP of a smartphone quantum-safe messaging application for French Special Forces

Picture taken during the experiments (150 participants from special forces)

Demonstration

Quantum-Safe Key Exchange
+ AES

Demonstration



https://cryptonext-security.com/images/demo.mp4

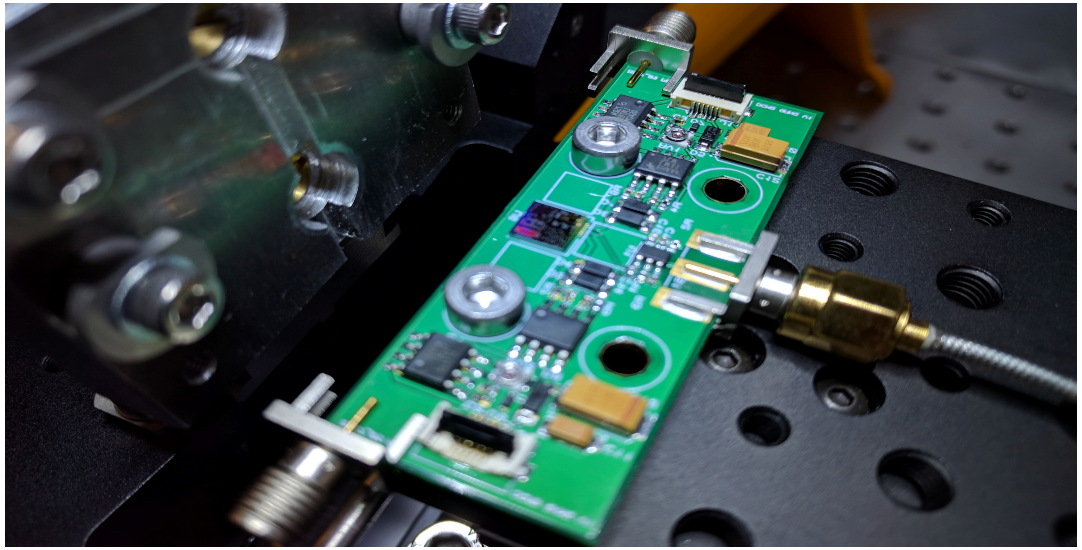
CRYPTONEXT SECURITY + KETS

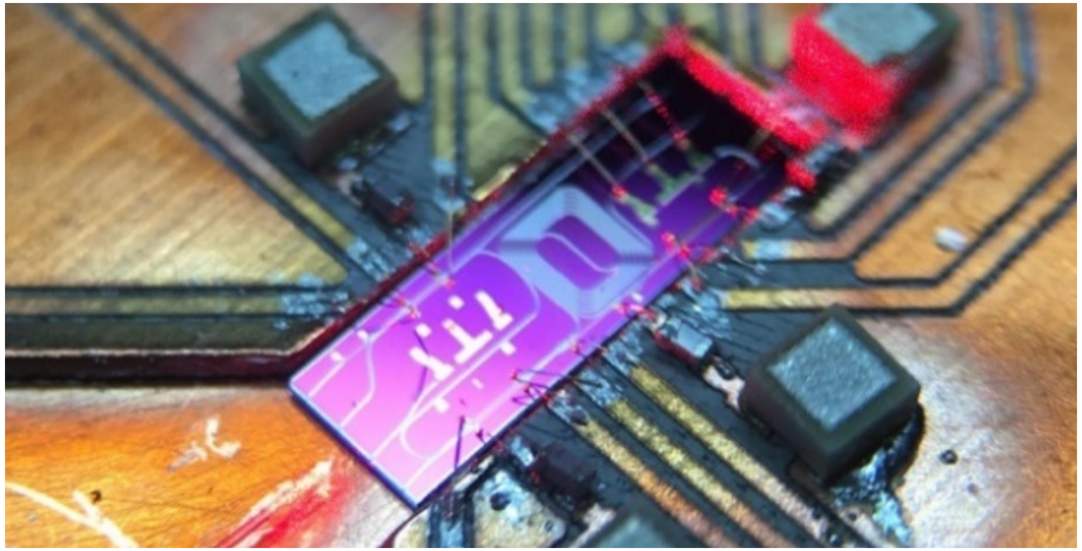
THE FUTURE OF SECURE COMMUNICATIONS

Winner 2018

UK's
Most Innovative
Small Cyber
Security Company

KETS is the first company with an on-chip quantum encryption solution.





DEPLOYMENT OF CRYPTONEXT SOFTWARE IN 2020 (Q1)

Leader Signature Electronique en France

DOCAPOST

Protection contre l'ordinateur quantique

CRYPTONEXT SECURITY

- Signature la plus complète et sécurisée du marché
- Solution hybride permettant de garder la conformité avec les normes actuelles
- Anticipation des nouveaux standards pour faire un choix de solution optimal
- Planification de la transition et évaluation de son impact


QUANTO NATION
CRYPTONEXT SECURITY
bpifrance
DEEP
TECH
WEEK
Quantum Cyber-Security : Impact And Challenges
March, 11th 2020 – 9h - 12h30
Bpifrance le HUB, 6-8 Bd Haussmann 75 009 Paris

CRYPTONEXT SECURITY

THEY SUPPORT US

CryptoNext is a spin-off from INRIA Paris and Sorbonne University incorporated in June 2019.

Incubated by Agoranov

Project selected by WILCO (2019, Digital accelerator) and Cyber@StationF (cybersecurity accelerator)

Member of the « Lab Quantique »

Hello Tomorrow Deep Tech Pioneers 2020 (5,000 applications from 128 countries) and Future 40 of Station F

Contact-Us !

ludovic.perret@cryptonext-security.com
Jean-Charles.Faugere@cryptonext-security.com
Frederic.de.Portzamparc@cryptonext-security.com

Web site: www.cryptonext-security.com

Is Quantum Supremacy changing everything ?

a « random » view from a « photon » guy

Sylvain Gigan

Le Lab Quantique Meet'up

Dec 17, 2019

Laboratoire Kastler Brossel
Physique quantique et applications

Sylvain.gigan@lkb.ens.fr

LightOn

sylvain@lighton.io

PIs:
Prof. Sylvain GIGAN
Dr. Hilton BARBOSA DE AGUIAR (JRC)

Postdocs
Dr. Mushegh RAFAYELYAN
Dr. Pauline BOUCHER
Dr. Bernhard RAUER
Dr. Michal DABROWSKI
Dr. Claudio MORETTI

PhD Students
Louisiane DEVAUD
Antoine BONIFACE
Jonathan DONG
Tom SPERBER
Julien GUILBERT
Saroch LEEDUMRONGWATTHANAKUN

Our Goal :
Understand and exploit the complexity of light propagation in complex media

DARPA
FET
FET-Open.
NIH
National Institutes
erc
European Research Council
Established by the European Commission
PROJET FINANCÉ PAR L'ANR
ANR
PROJECT FUNDED BY THE ANR

Alumni

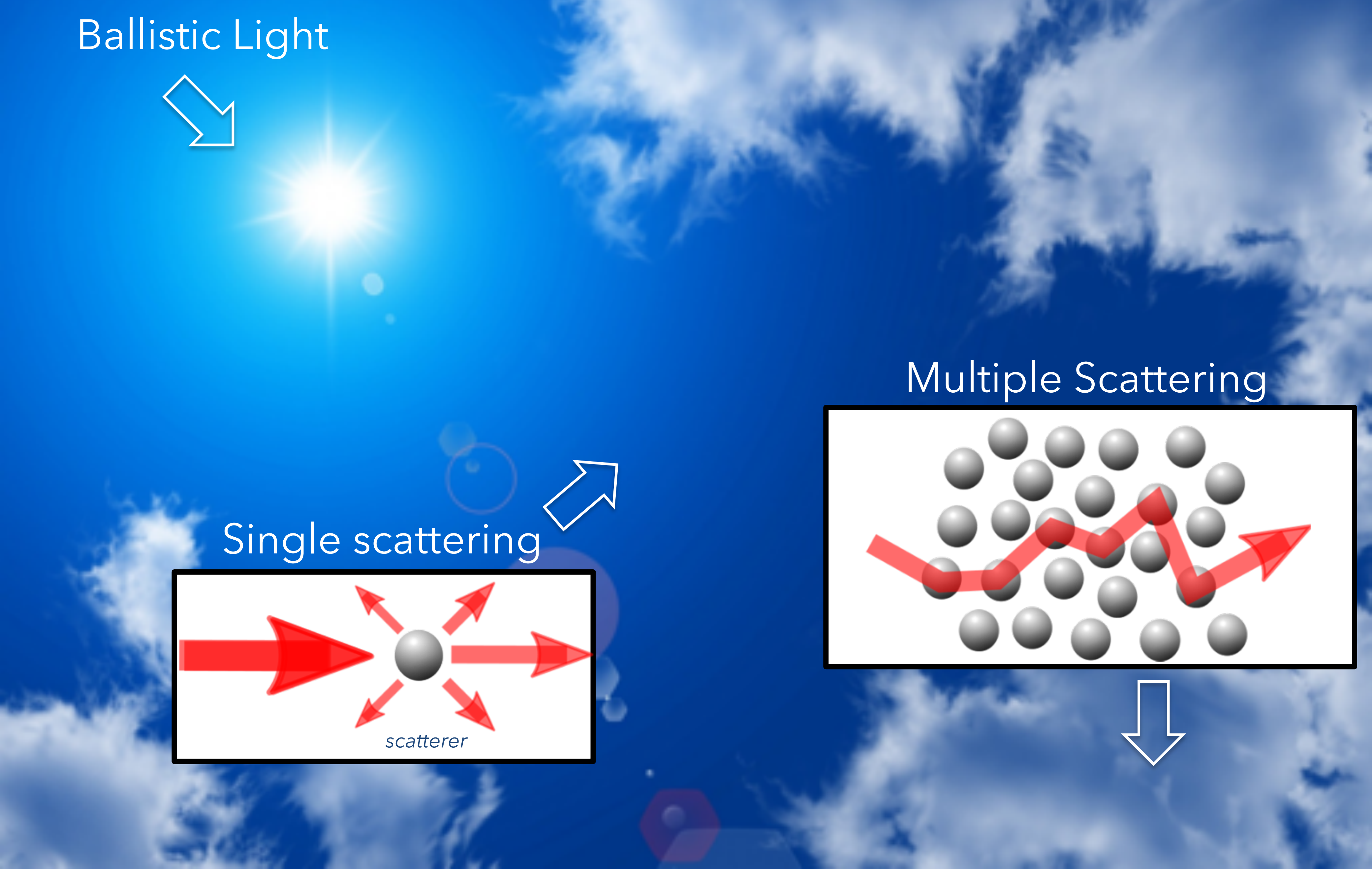
PhDs:
S.Popoff (CNRS)
D.Andreoli
P.Bondareff
T.Chaigne (CNRS)
H.Defienne
M. Mounaix
B. Blochet

Postdocs:
D.Martina
G. Volpe (UCL)
J.Bertolotti (U.Exeter)
O.Katz (HUJI)
R. Savo (ETH)
T. Juffman (U. Vienna)
I Gusachenko (cailabs)

Main national and International Collaborations

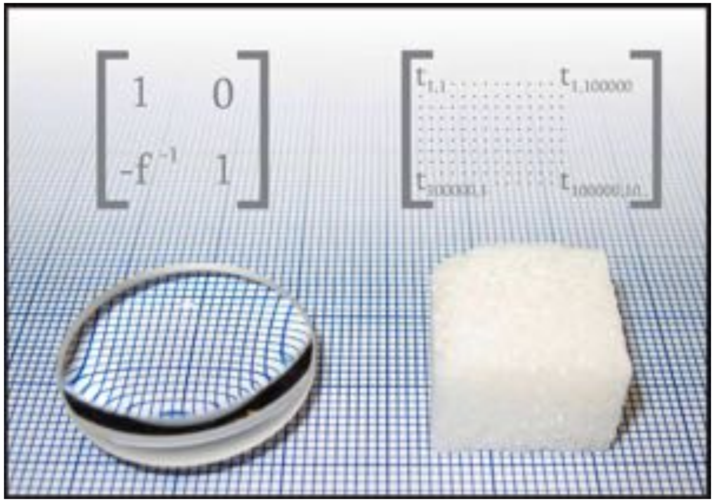
L. Bourdieu (IBENS)
F..Krzakala (LPENS)
M. Fink, P. Sebbah
S. Bidault, S. Grésillon
R. Carminati, R. Pierrat (ESPCI ParisTech)
F. Soldevila, E. Tajahuerce, J. Lancis (Castellon)
E. Bossy (UJF Grenoble)
M. Paternostro (U. Belfast)
R. Di Leonardo (U. Roma)
R.Piestun (U. Colorado, Boulder)
O. Muskens (Southamton)
S. Rotter (TU Wien)
S.Brasselet (Institut Fresnel)

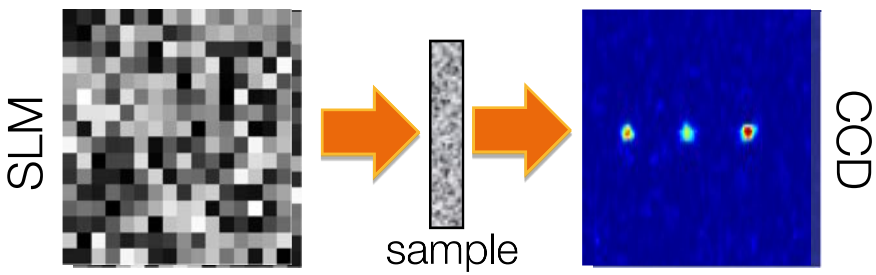
Scattering


Ballistic Light
Single scattering
scatterer
Multiple Scattering

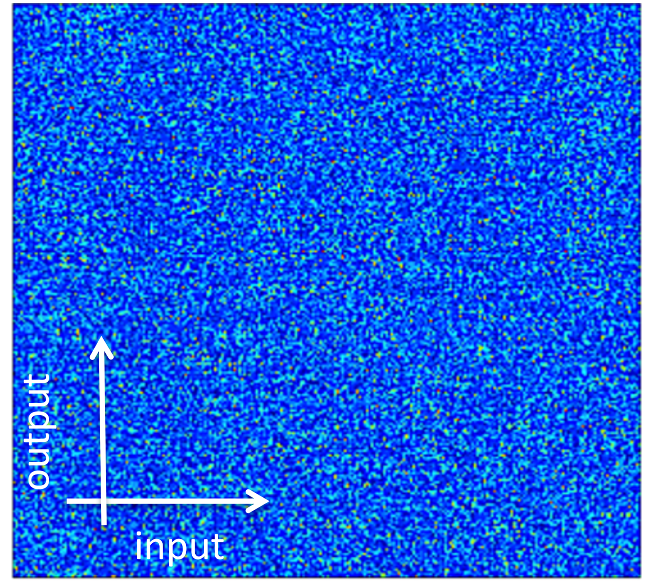
Controlling light propagation in complex media

… measuring the transmission matrix





Popoff et al. Phys. Rev. Lett. 104,100601 (2010)



Transmission matrix
of a complex mediim

Propagation = perfect (random) mixing of information

Idea: borrow from Computer Science to **take advantage** of disorder

A counter-intuitive lesson from signal processing and information theory

Randomness can be optimal to analyze information

Propagation of light through a disordered medium

=

multiplication by a complex i.i.d. random matrix

« Random projections »

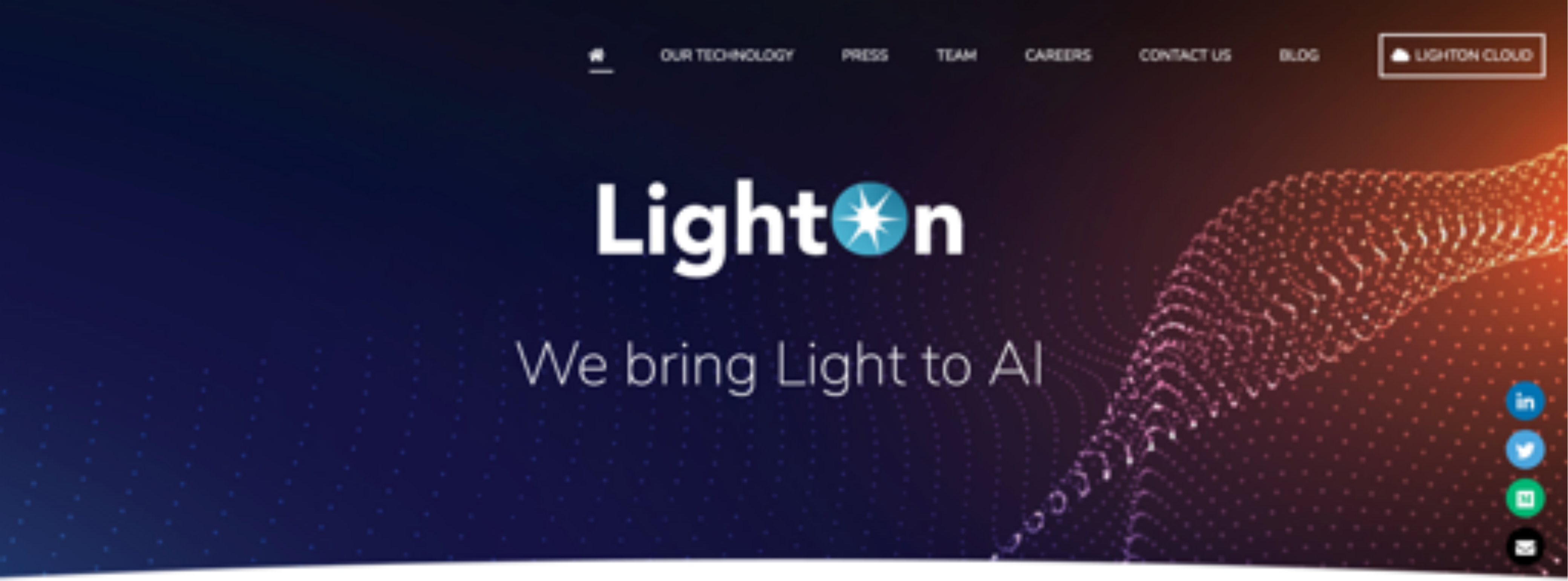
=

A **universal** operation

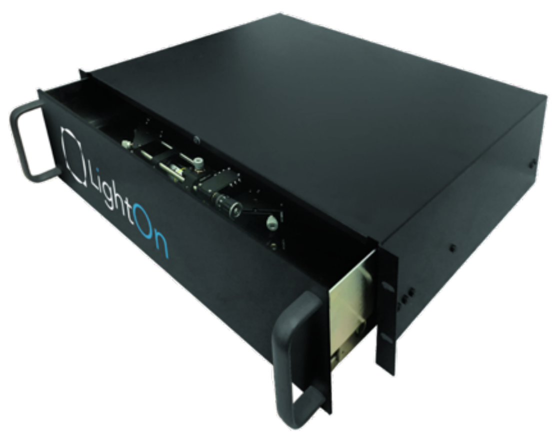
Compressive sensing
Candès and Tao (2006) [>4800 citations]

Machine Learning
Huang et al. (2006) [3500 citations]

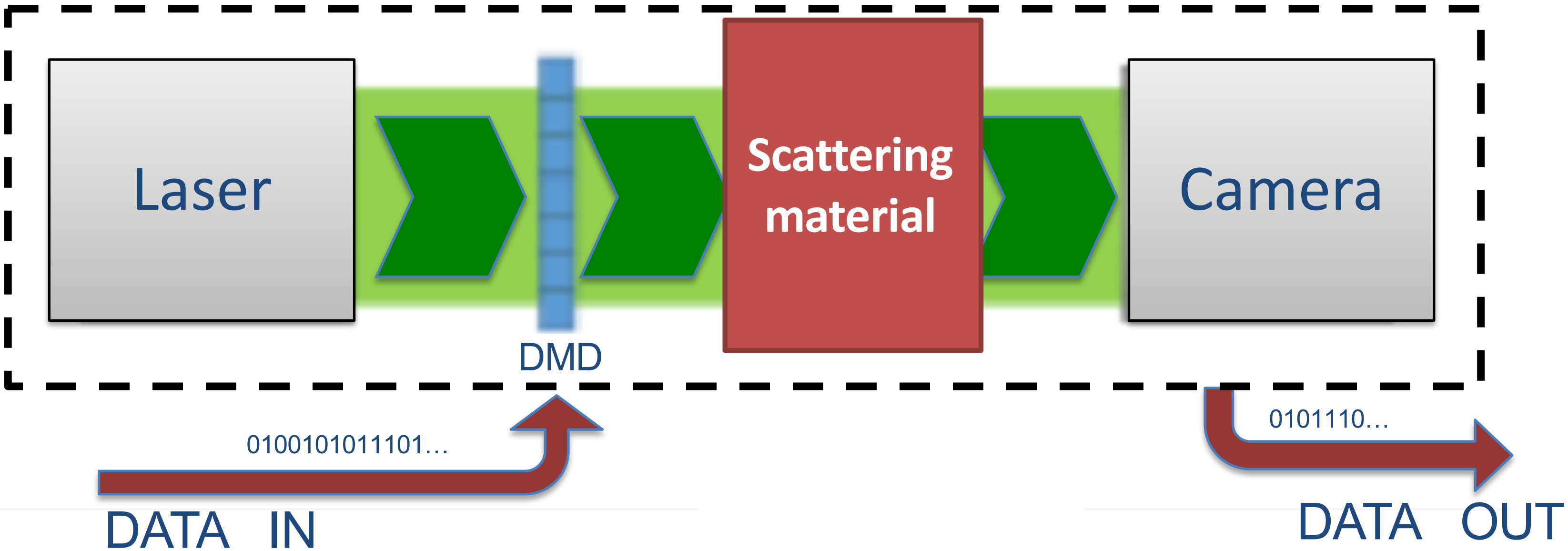
« randomized » Linear Algebra
Candès and Recht, 2009 [2300 citations]



LightOn is a technology company developing novel optics-based computing hardware.



Optical Computing for Large scale AI



Why is it interesting ?

EXTRA-LARGE & **SUPER-FAST**

H of size higher than $10^6 \times 10^6$ (TBs of memory)

kHz operation → 10^3 such multiplies / s

Equivalent 10^{15} operations / s : You would need a *Peta-scale* computer to do the same !

What about Q. Supremacy ?

- Same goal
- Different applications
- There is no silver bullet!
- A strong common message : there is an alternative to Silicon

« The world is rapidly running out of computing capacity »

Satya Nadella, CEO Microsoft, Jan'18

SCALABILITY ?

https://www.youtube.com/watch?v=Ak7HPuuJ1Ow

SUSTAINABILITY ?

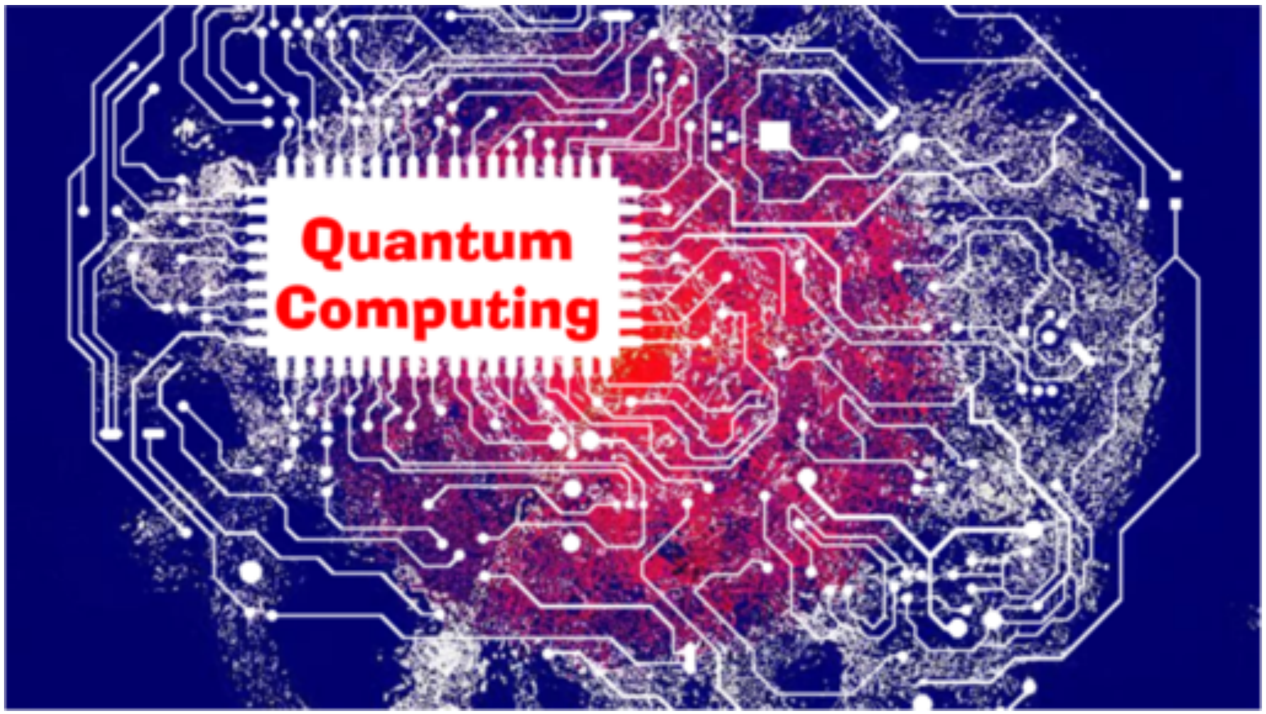
The Guardian

'Tsunami of data' could consume one fifth of global electricity by 2025

11 Dec 2017

Can you do more than classical computing with a complex medium ?

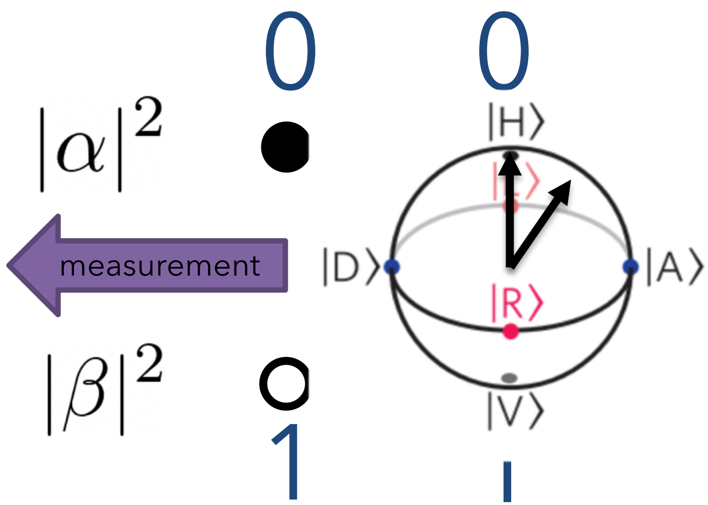
… actually YES



Laboratoire Kastler Brossel
Physique quantique et applications

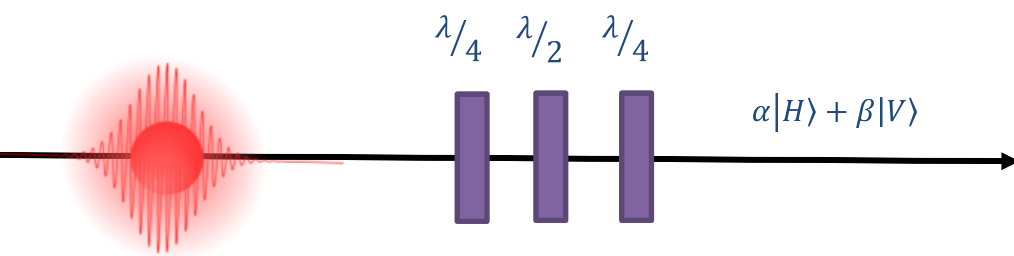
Photons for quantum information

Bits of information can be encoded on optical fields



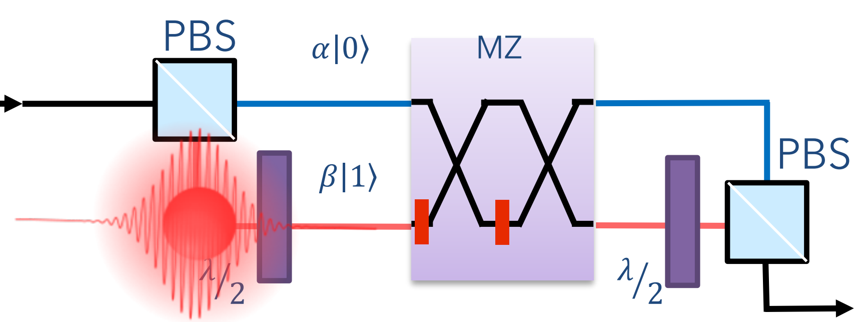
Quantum bit encoded in polarization

Single Photons

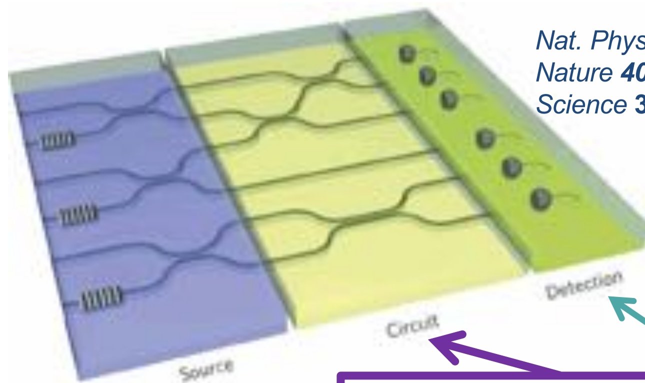


Single qubit processing

Polarization to path encoding



Photonic quantum information processing



Nat. Phys. **8**, 285-291 (2012)
Nature **409**, *46–52 (2001)*
Science **349**, 6249, 711-716 (2015)

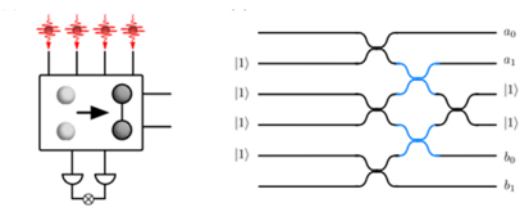
Single photon detections

Non-classical light

Reconfigurable linear transformation

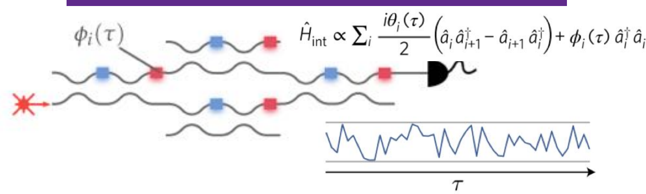
Several processing tasks on the same platform

Quantum Computation



J. Carolan, *et al.*, *Science* **349**, 711-716 (2015)

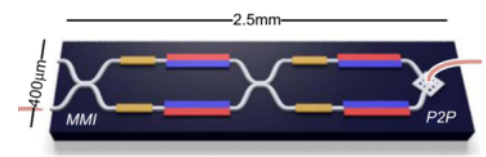
Quantum Simulation/ Walk



N. C. Harris, et al., Nat. Phot. **11**, 447 (2017)

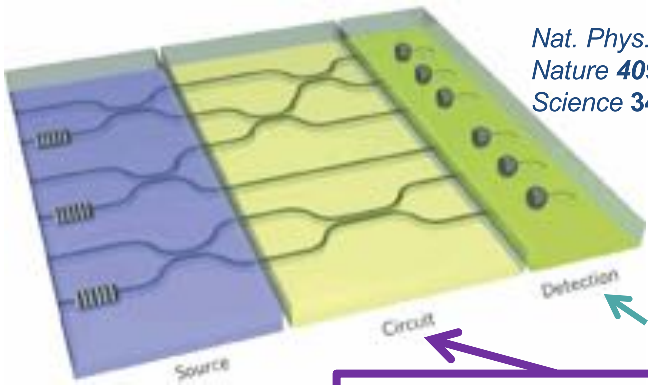
Quantum Communication

BB84 - POLARIZATION



P. Sibson, et al., Optica. **4**(2), 172 (2017)

Photonic quantum information processing



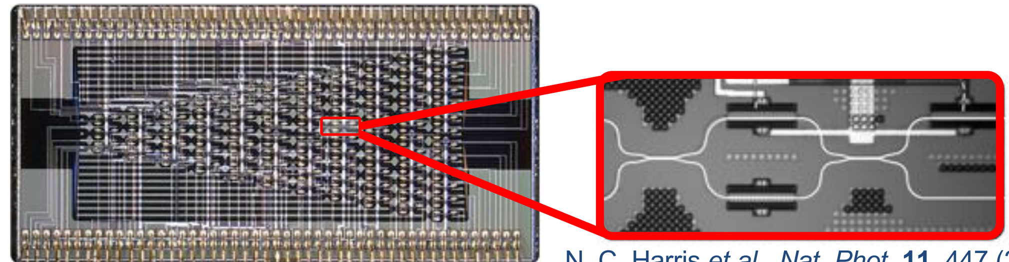
Nat. Phys. **8**, 285-291 (2012)
Nature **409**, 46–52 (2001)
Science **349**, 6249, 711-716 (2015)

Single photon detections

Non-classical light

Reconfigurable linear transformation

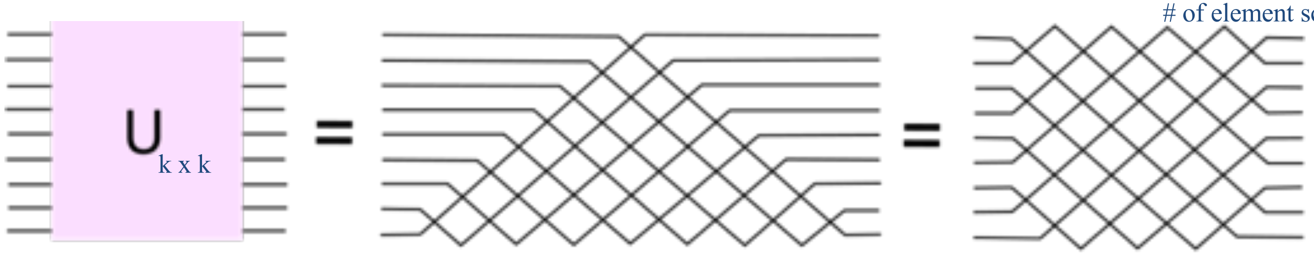
Integrated photonic circuit on chip

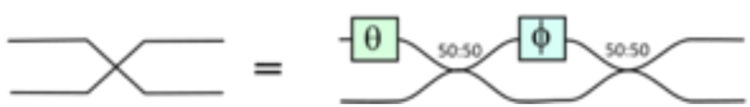


N. C. Harris *et al.*, *Nat. Phot.* **11**, 447 (2017)

Cascade of 2 x 2 MZ interferometers

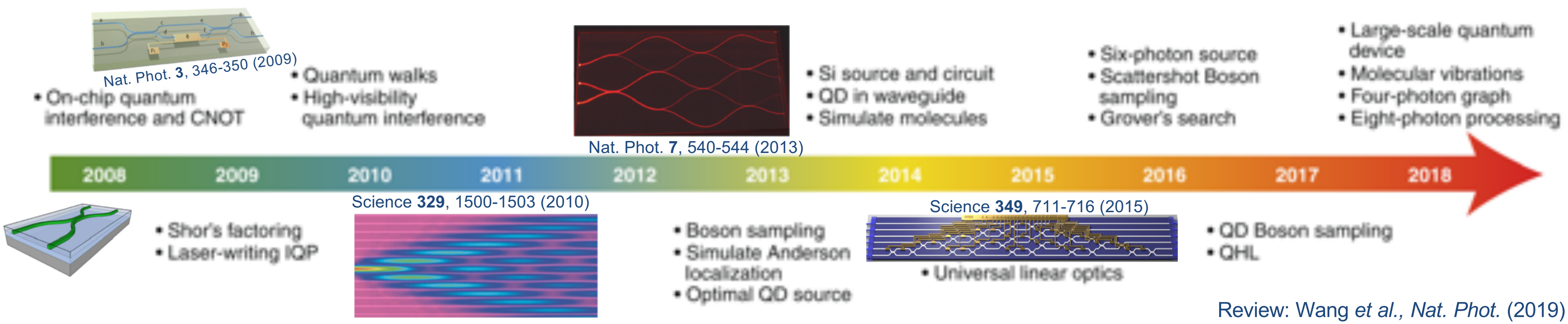
of element scales $O(k^2)$



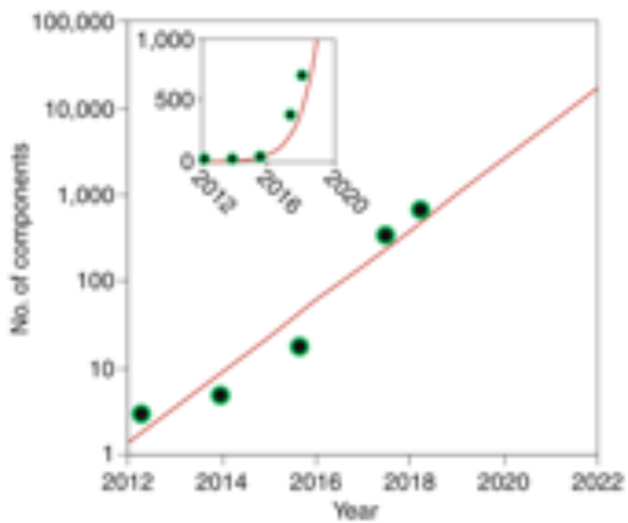


M. Reck, *et al.*, *PRL* **73**, 58 (1994)
W.R. Clements, *et al.*, *Optica* **3**, 1460 (2016)

Integrated photonic quantum information processing



Review: Wang *et al.*, *Nat. Phot.* (2019)



Requirements

- Scalability
- Low loss
- Full programmability

Review: *Optica* **5**, 1623 (2018)

Limitations

- Rely on single-mode waveguides
- Mixing of a few tens of modes only

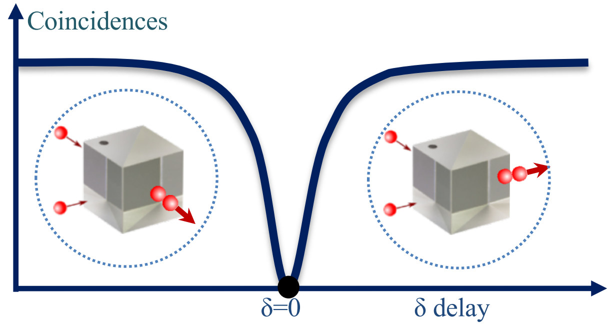
Complexity of Quantum Interference

Two-photon interference

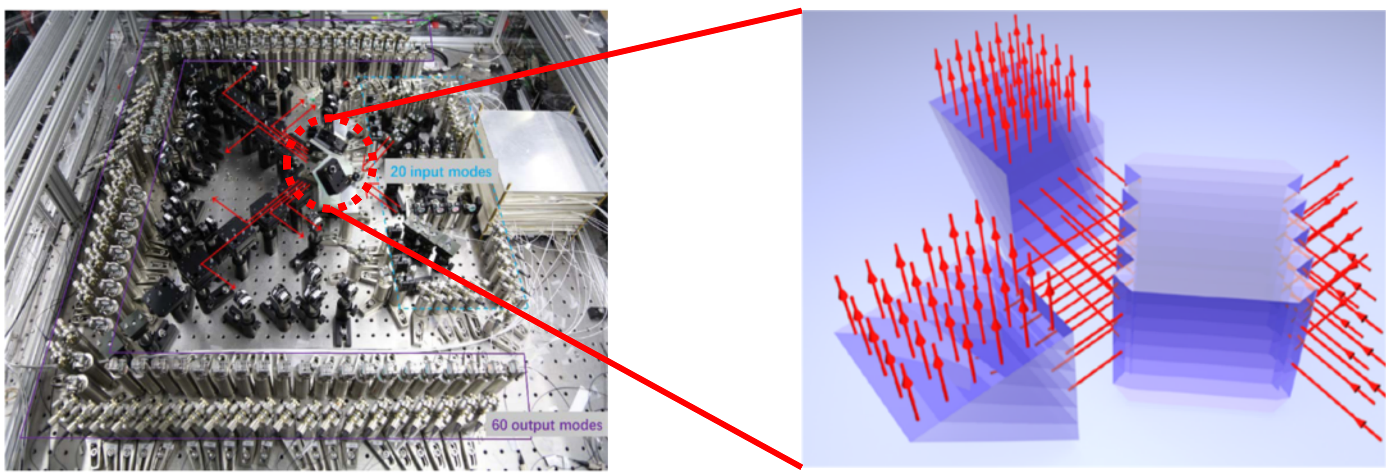
C. K. Hong, Z. Y. Ou, and L. Mandel, *PRL*, **59** (18), 2044 (1987)

$$\mathrm{BS} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}$$

$$\left|\mathrm{Perm}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right|^2 = |ad + bc|^2$$

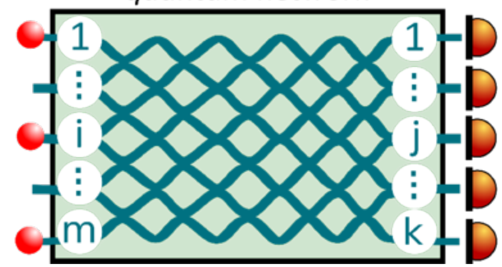


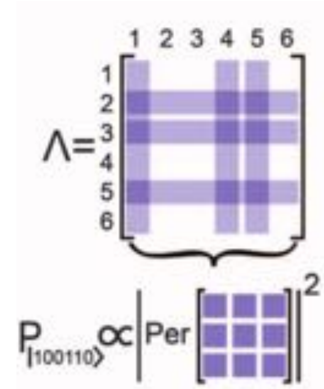
20 single photons fed into 60-mode interferometer



H.Wang, et al., Arxiv:1910.09930 (to appear in PRL)

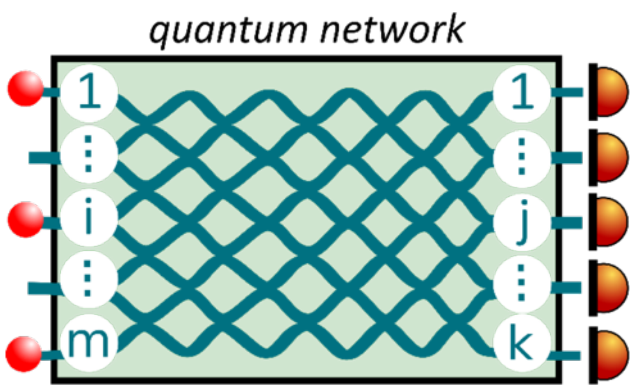
Boson Sampling



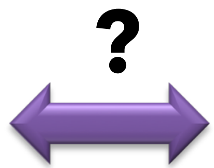


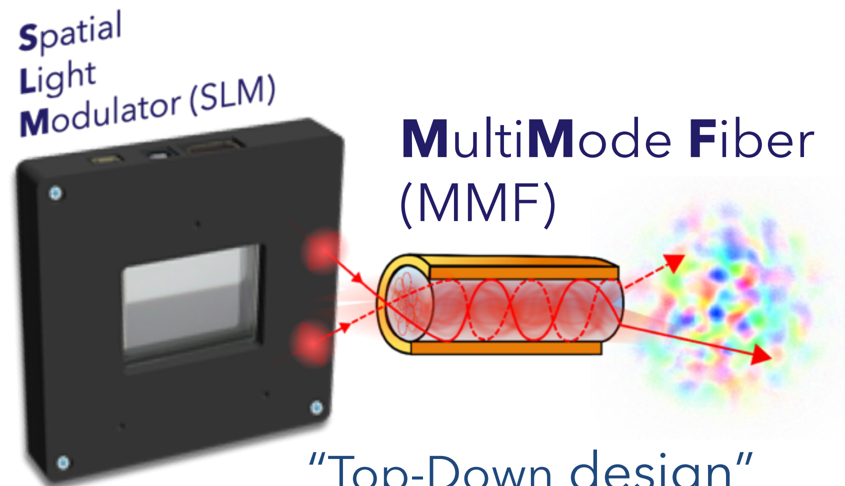
S. Aaronson and A. Arkhipov, STOC'11 (2011)
J. B. Spring, *et al.*, *Science* **339**, 798 (2013)

Programmable linear circuit with a multimode fiber



"Bottom-Up design"



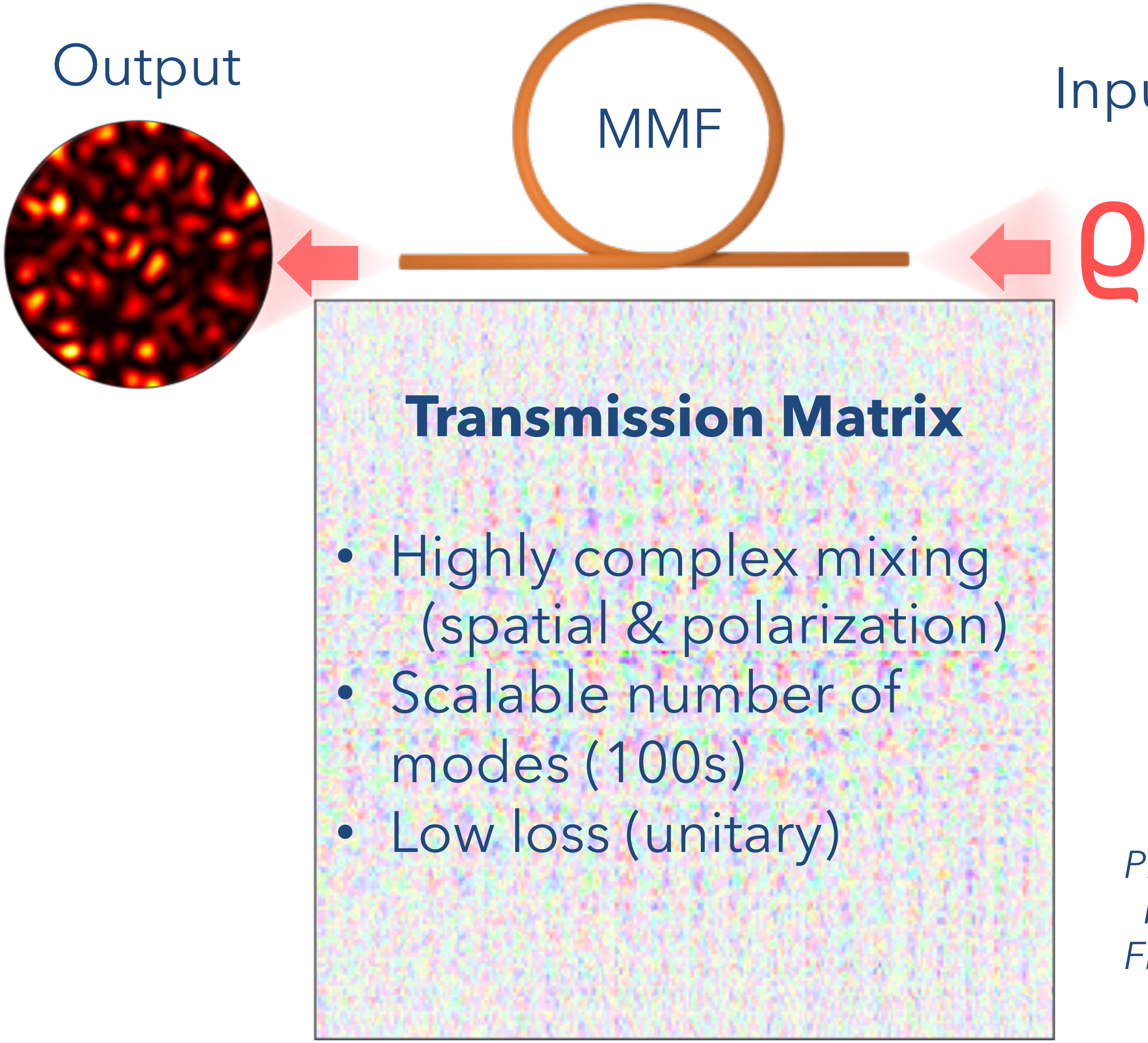


"Top-Down design"

The goal!

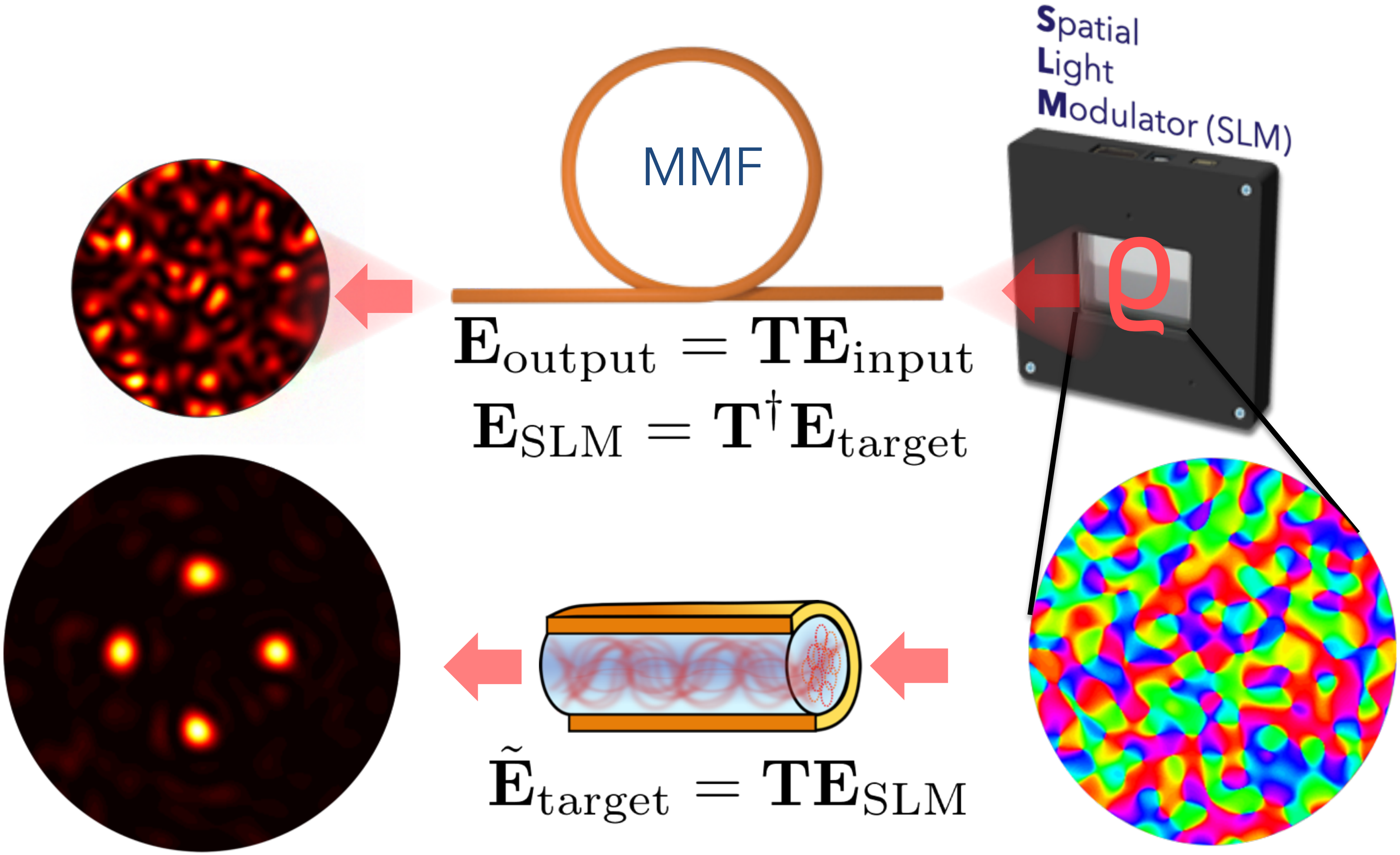
$$\begin{bmatrix} \hat{b}_1 \\ \hat{b}_2 \\ \hat{b}_3 \\ \vdots \\ \hat{b}_k \end{bmatrix} = \begin{bmatrix} L_{11} & L_{12} & L_{13} & \cdots & L_{1m} \\ L_{21} & L_{22} & L_{23} & & \\ L_{31} & L_{32} & L_{33} & & \\ \vdots & & & \ddots & \\ L_{k1} & & & & L_{km} \end{bmatrix} \times \begin{bmatrix} \hat{a}_1 \\ \hat{a}_2 \\ \hat{a}_3 \\ \vdots \\ \hat{a}_m \end{bmatrix}$$

Complex mixing within a Multimode Fiber (MMF)



Ploschner, et al.,
Nat. Phot. **9**, 529 (2015)
Flaes, et al.,
PRL **120**, 233901 (2018)

Programmability with Wavefront Shaping



$$\mathbf{E}_{\text{output}} = \mathbf{T}\mathbf{E}_{\text{input}}$$

$$\mathbf{E}_{\text{SLM}} = \mathbf{T}^{\dagger}\mathbf{E}_{\text{target}}$$

$$\tilde{\mathbf{E}}_{\text{target}} = \mathbf{T}\mathbf{E}_{\text{SLM}}$$

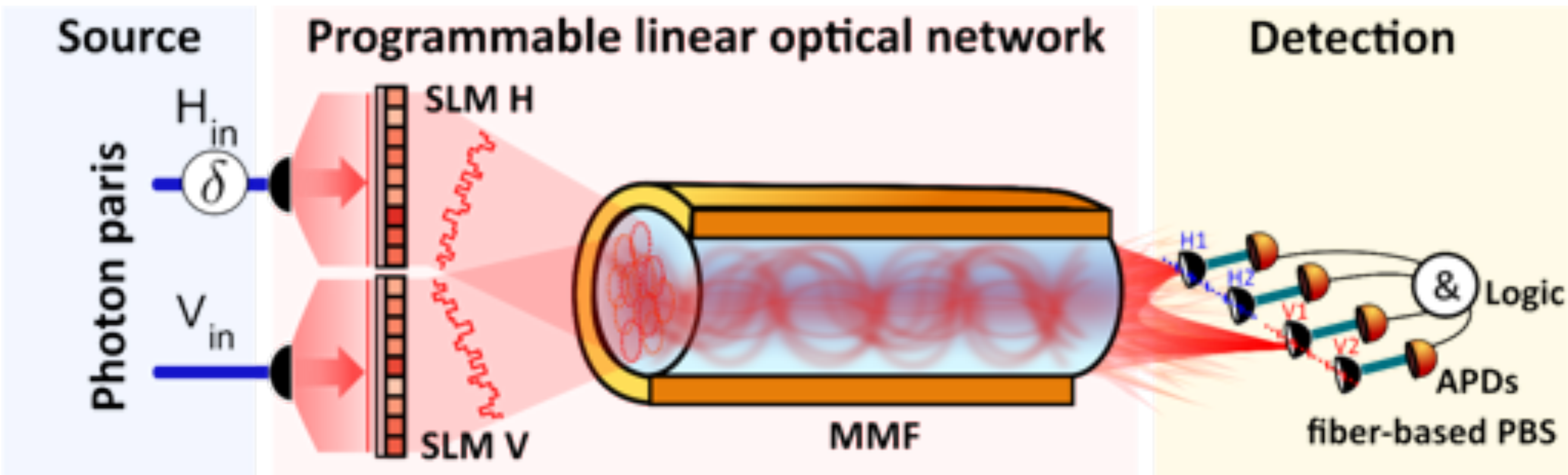
Complex Circuits? Yes we can !

QUEEN'S UNIVERSITY BELFAST

Luca Innocenti

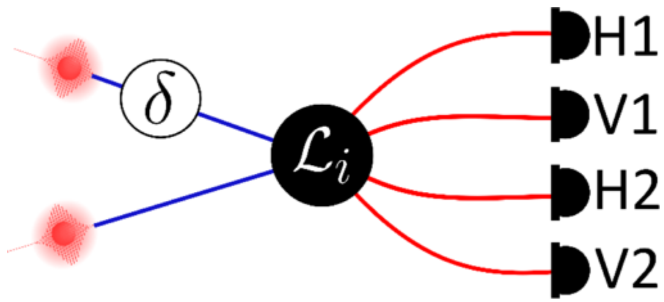
Alessandro Ferraro

Mauro Paternostro



We can implement any 2x4 transform for 2 photons
2 spatial modes x 2 polarizations

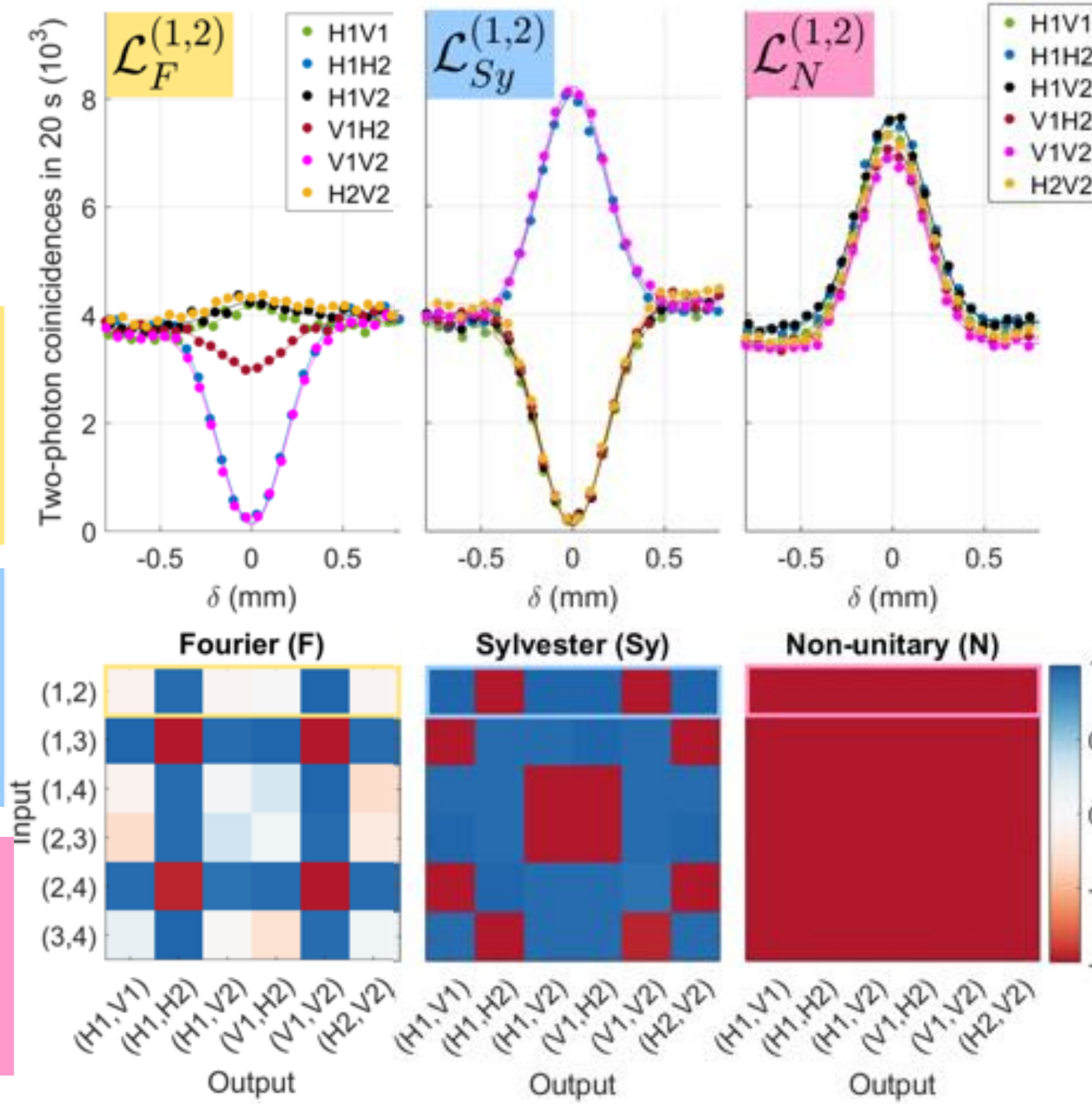
Some examples of circuits



Fourier $U_F = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix}$

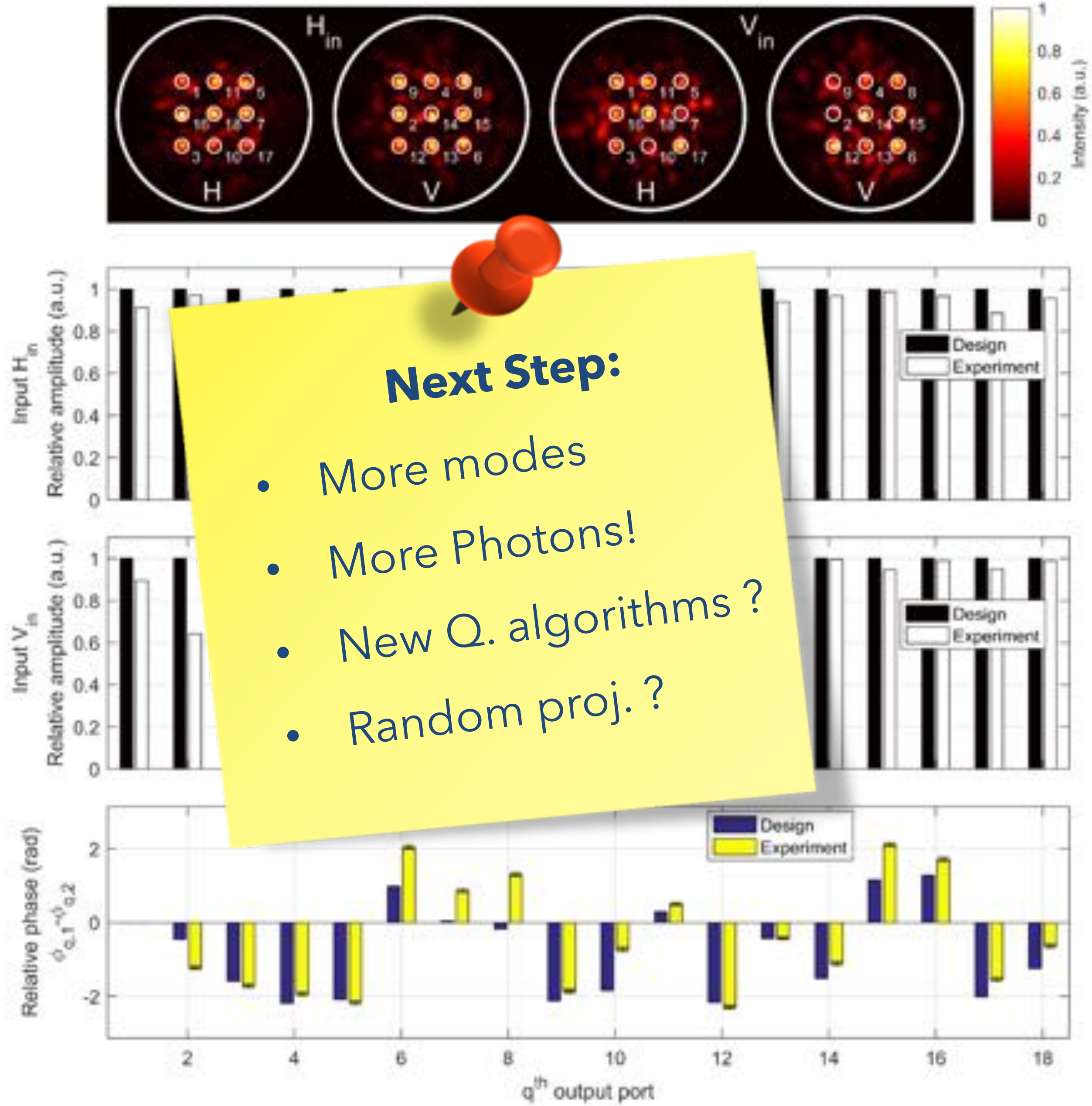
Sylvester $U_{Sy} = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$

Non-Unitary $\mathcal{L}_N = \eta\begin{bmatrix} 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$



Leedumrongwatthanakun S., *et al.* Nature Photonics (2019)

A scalable platform



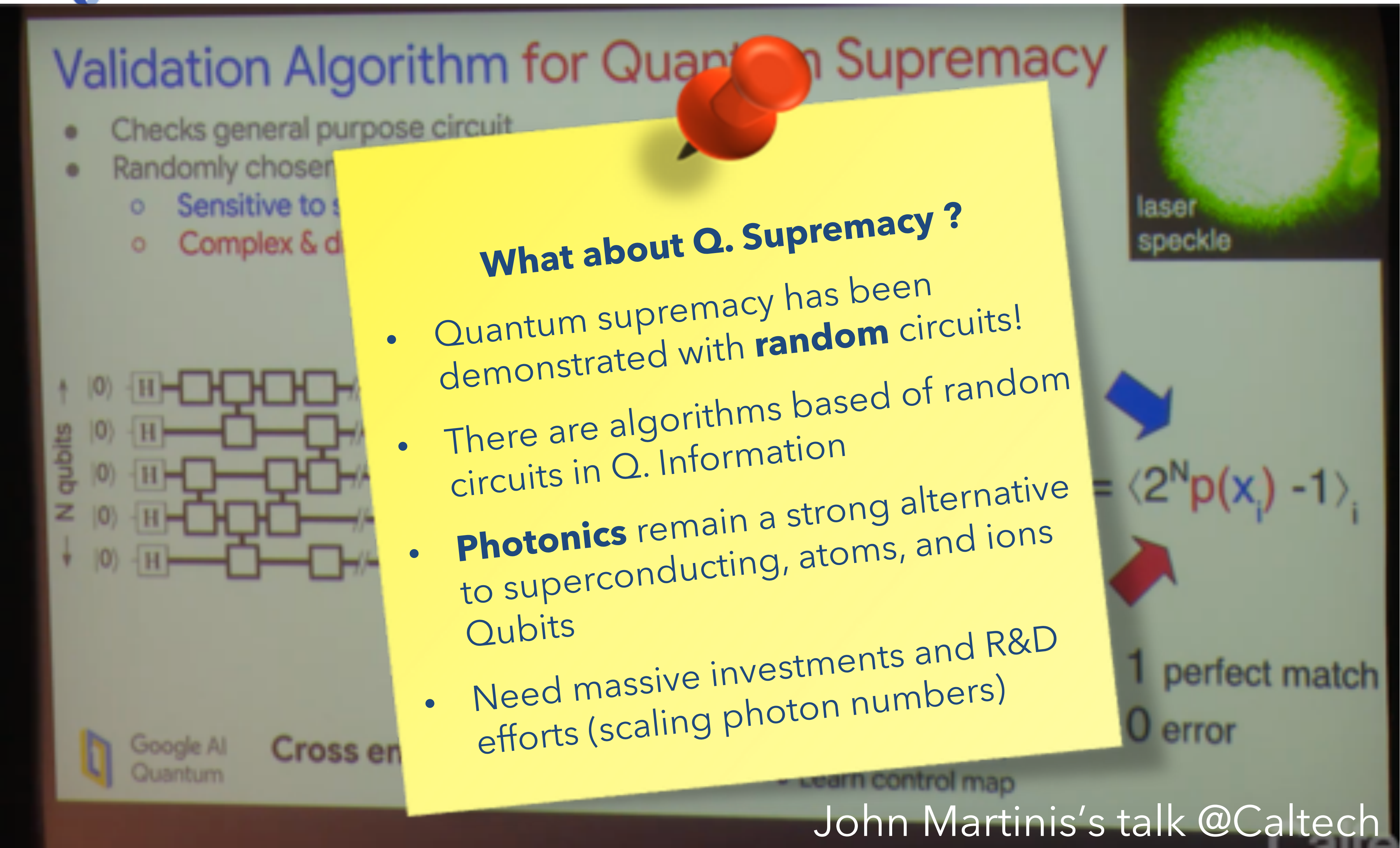
Next Step:

- More modes
- More Photons!
- New Q. algorithms ?
- Random proj. ?

What about Google AI Quantum ?

What about Q. Supremacy ?

- Quantum supremacy has been demonstrated with **random** circuits!
- There are algorithms based of random circuits in Q. Information
- **Photonics** remain a strong alternative to superconducting, atoms, and ions Qubits
- Need massive investments and R&D efforts (scaling photon numbers)



John Martinis's talk @Caltech

Thanks to my coworkers and collaborators

Thank you for your attention !

Mail : sylvain.gigan@lkb.ens.fr
Webpage: www.lkb.ens.fr/gigan

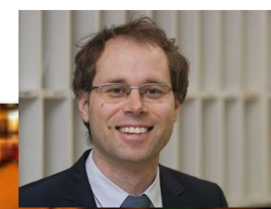
If you are interested in the field :

REVIEWS OF MODERN PHYSICS

Recent Accepted Authors Referees Search Press About

Light fields in complex media: Mesoscopic scattering meets wave control

Stefan Rotter and Sylvain Gigan
Rev. Mod. Phys. **89**, 015005 – Published 2 March 2017



Stefan Rotter
(TU Wien)